Mujeres Activistas XSL

# Protocolo básico de manejo de evidencias en caso de sospecha o identificación de Violencias de Género Facilitadas por Tecnologías (VGFT)

## Hoja de ruta hacia una forénsica digital feminista


# Créditos

## Comunidad de aprendizaje:

Nerissa José, Aguilera Arteaga
María Ángela, Petrizzo Páez
Jesús, Rojas Álvarez
Manuela Yasmin, Capó Sisco
Katiuska Elimar, Duque Bohórquez
Prissilla, Noguera Mendoza
Raquel Daneli, Piña Rodríguez
Gabriela, López González
Luisana del Valle, Parejo Ramírez
Anavelyz, Pérez

## Diseño e ilustración:

Sandra, Triana Duarte
@sandra_triana77

## Maquetación:

Manuela Yasmin, Capó Sisco
@manuela_yasmin_

**@activistassl**
**contacto@activistasxsl.org**
**http://activistasxsl.org**

Mujeres
Activistas
XSL

**Caracas, marzo 2026**

# Contenido

# Presentación

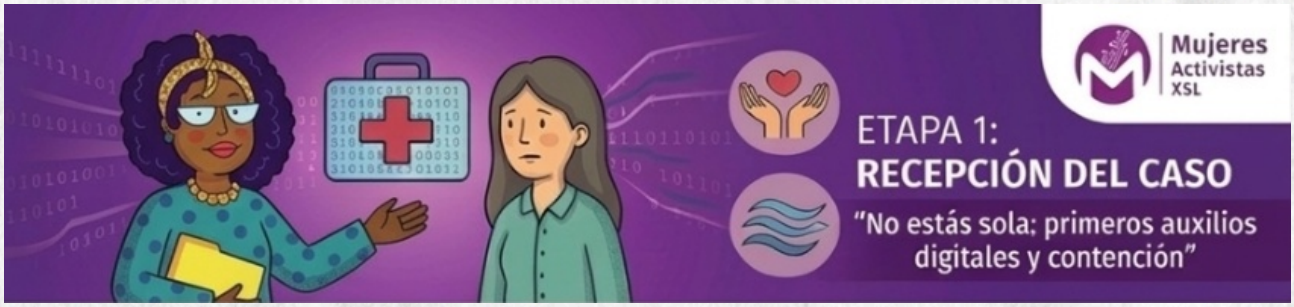
El presente protocolo es el resultado de un proceso colectivo de formación y reflexión. Surge tras la realización del taller de "Fundamentos de Informática Forense con Perspectiva Feminista", en el que 8 mujeres activistas, abogadas, técnicas y defensoras de derechos humanos se formaron en conceptos básicos de forénsica digital, identificación, preservación y análisis de evidencia digital, con el objetivo de fortalecer los procesos de acompañamiento a víctimas y sobrevivientes de **Violencias de Género Facilitadas por Tecnologías (VGFT).**

Este documento retoma el proceso de acompañamiento desarrollado por Mujeres Activistas por el Software Libre presentado en la **Guía 3: Lo que debes hacer en caso de ser víctima de violencias digitales** y lo articula con los conocimientos técnicos adquiridos durante el taller, para construir una hoja de ruta que integre la forénsica digital desde una perspectiva feminista: *centrada en la sobreviviente, respetuosa de sus tiempos y decisiones, y comprometida con la no revictimización.*

**El protocolo se estructura en torno a las 5 etapas del proceso de acompañamiento identificadas por Activistas XSL en la siguiente Figura 1:**

**Figura 1: Etapas del proceso de acompañamiento identificadas por Activistas XSL**


A cada etapa se incorporan ahora consideraciones éticas, técnicas y legales derivadas de la formación en forénsica digital, así como herramientas concretas para la identificación, preservación y análisis de evidencia digital, siempre en diálogo con el marco legal venezolano vigente.




### 1.1. Primer contacto y acogida

**Objetivo:**

Establecer un vínculo de confianza, garantizar la confidencialidad y realizar una primera evaluación de la situación.

**Acciones:**

- ***Escucha activa y validación:*** Recibir a la sobreviviente en un espacio seguro, sin juicios. Frase clave: "No es tu culpa, siempre es culpa del agresor".
- ***Explicación del proceso:*** Informar de manera clara y sencilla sobre qué implica el acompañamiento, qué podemos ofrecer (apoyo técnico, asesoría legal, contención emocional) y qué no (terapia psicológica profesional, representación judicial directa si no contamos con abogada disponible). Es fundamental no generar falsas expectativas.
- ***Confidencialidad y anonimización:*** Explicar que toda la información será tratada de forma confidencial. Desde este primer momento, se debe iniciar un proceso de anonimización de datos personales (nombre, cédula, contactos, ubicación exacta) separándolos de la descripción del caso y vinculándolos mediante un código interno. Los archivos sensibles deben ser cifrados.

### 1.2. Documentación inicial de la agresión

**Objetivo:**

Recopilar la mayor cantidad de información posible sobre los hechos, de forma ordenada, para facilitar el análisis posterior.

**Acciones:**

- ***Uso del cuadro de sistematización de evidencia:*** Entregar a la sobreviviente (o ayudar a llenar) el cuadro propuesto por ActivistasXSL, que permite registrar de forma sistemática cada evento de violencia:

| Fecha Hora | ¿Qué Ocurrió? | Evidencia de lo que ocurrió | Identificación de posible responsable | ¿Por qué crees que lo hizo? | Red o redes sociales desde donde se realiza la agresión | Evidencia que no tienes y consideras importante | Acciones emprendidas |
|---|---|---|---|---|---|---|---|
| La fecha y hora del evento | Descripción de lo ocurrido | Identificar la evidencia que ya se tiene, adjuntar una captura de pantalla, pdf, una publicación, un correo, un mensaje de voz. Colocar el nombre del archivo. | Para cada evento identifica a la posible persona responsable | Explicar las razones por las que cree que es o son responsables. Ejemplo: Porque Fulanito me envió un mensaje el 3 de enero diciéndome que si no le contesto publicaría todas mis fotos. | Capturas de pantalla y enlaces de la red(es) social(es) desde donde se realizó la agresión | Hacer una lista de posibles evidencias que no tienes pero que puede ser útil. Por ejemplo: El 5 de febrero Fulanito le envió un mensaje a mi mejor amiga diciéndole que me avisara que publicaría todas mis fotos. | Indicar si se realizó algún trámite, acciones o denuncias ante órganos competentes o ante alguna plataforma de red social |
| | | | | | | | |
| | | | | | | | |

**Cuadro 1. Registro de evidencias**

***Indicaciones para la recolección de evidencia:***

Instruir a la sobreviviente sobre cómo guardar las pruebas sin alterarlas:

- Tomar capturas de pantalla completas que incluyan la URL, la fecha y la hora visibles.
- Guardar las publicaciones como PDF (desde el navegador, opción "Imprimir" y "Guardar como PDF").
- Conservar audios, vídeos, mensajes en su formato original.
- En caso de llamadas o mensajes de texto, anotar número, fecha y hora.
- Guardar los enlaces de los perfiles desde los que se realiza la agresión y de las publicaciones específicas.
- Crear una carpeta digital con toda esta evidencia y realizar una copia de seguridad (respaldo en la nube, disco externo o, si es posible, en un dispositivo seguro de la persona de confianza).

***Acompañamiento en la documentación**:*

Si el proceso de recolección resulta revictimizante o abrumador para la sobreviviente, ofrecer ayuda de una persona de confianza o, si es posible, que una integrante del equipo de acompañamiento realice esta tarea junto a ella, respetando siempre su ritmo y sus límites.

### 1.3. Evaluación de riesgos inmediatos

**Objetivo:**

Identificar situaciones de peligro inminente que requieran medidas urgentes de protección.

**Acciones:**

- Identificar amenazas explícitas de daño físico.
- Detectar si el agresor podría tener acceso físico a los dispositivos de la sobreviviente o si existe sospecha de software de monitoreo (stalkerware) en su teléfono o computadora.
- Evaluar si se ha publicado información personal sensible (dirección, lugar de trabajo, datos de familiares) que ponga en riesgo su integridad física.
- Preguntar si existe violencia física previa en el ámbito offline.

### 1.4. Primeros auxilios digitales

**Objetivo:**

Implementar medidas básicas de seguridad digital para proteger a la sobreviviente mientras se diseña una estrategia más completa.

**Acciones (explicar paso a paso y acompañar si es necesario):**

- ***No responder al agresor:*** Explicar que responder puede empeorar la situación y que el silencio no es una señal de debilidad.
- **Cambio de contraseñas:** Ayudar a generar contraseñas seguras y únicas para cada cuenta. Recomendar el uso de un gestor de contraseñas.
- **Activación de la autenticación en dos factores (2FA):** Guiar en la activación de este mecanismo en todas las plataformas donde sea posible (correo, redes sociales, mensajería).
- **Revisión de la configuración de privacidad:** Revisar quién puede ver las publicaciones, quién puede contactar a la sobreviviente, y ajustar la configuración para mayor seguridad.
- **Cierre de sesiones en dispositivos desconocidos:** Desde la configuración de seguridad de cada plataforma, revisar y cerrar sesiones activas en dispositivos que no reconozca.
- **Desconexión temporal:** Recomendar tomarse un tiempo de descanso de las redes sociales si esto contribuye a su bienestar emocional, pero sin caer en la autocensura ni en la idea de que debe abandonar el espacio digital.
- **Reportes inmediatos a plataformas:** Si la agresión es urgente (ej. difusión de imágenes íntimas), guiar en el proceso de reporte en la plataforma correspondiente (ver Anexo 1).


**2.1. Análisis conjunto de la información**

**Objetivo:**

Analizar la información recopilada en la etapa de recepción para comprender la naturaleza del caso, identificar los tipos de violencia y determinar las necesidades y expectativas de la sobreviviente.

**Acciones:**

- ***Revisión del cuadro de sistematización:*** Analizar juntas la información registrada.
- ***Identificación de las violencias ejercidas:*** Clasificar los hechos según los tipos de violencia reconocidos en la legislación venezolana, especialmente la violencia informática y el uso de TIC como agravante de otras formas de violencia (acoso, hostigamiento, violencia política, etc.).
- ***Comprensión de las expectativas:*** Preguntar a la sobreviviente: ¿Qué esperas de este acompañamiento? ¿Qué sería para ti una resolución satisfactoria? Las respuestas pueden ir desde "que pare el acoso", pasando por "que se eliminen las imágenes", hasta "que el agresor sea llevado ante la justicia". Es clave respetar sus deseos y no imponer objetivos.
- ***Evaluación de la capacidad de respuesta:*** Determinar si el equipo de acompañamiento cuenta con las herramientas técnicas y legales para abordar el caso o si es necesario derivar a otras organizaciones o especialistas.

**2.2. Analisis Digital Forense Feminista**

**Objetivo:**

Aplicar los conocimientos básicos de forénsica digital adquiridos en el taller para realizar una primera exploración técnica del caso, sin necesidad de ser peritas expertas, pero con la rigurosidad necesaria para no contaminar evidencia.

**Niveles del análisis:**

**Nivel 1: Básico (lo que podemos hacer nosotras con la formación recibida):**

- ***Verificación de metadatos básicos:*** Usar herramientas sencillas (visores de propiedades de archivo, páginas web como exifdata.com) para revisar metadatos de imágenes o vídeos que la sobreviviente haya recibido o descargado (fecha de creación, dispositivo, posible geolocalización).
- ***Revisión de registros de actividad de cuentas:*** Ayudar a la sobreviviente a solicitar y revisar los archivos de datos de sus cuentas principales (ej. Google Takeout, datos de iCloud, Meta). Esto permite identificar inicios de sesión no reconocidos, dispositivos vinculados o actividad sospechosa que pueda confirmar si la cuenta ha sido comprometida .
- ***Identificación visual de aplicaciones maliciosas en Android:*** En dispositivos Android, realizar una revisión guiada para identificar aplicaciones con permisos excesivos (acceso a ubicación, cámara, micrófono, contactos) que la víctima no recuerde haber instalado, o configuraciones que indiquen la instalación de aplicaciones de fuentes desconocidas .
- ***Análisis básico de enlaces y perfiles falsos:*** Usar técnicas de OSINT (Open Source Intelligence) básicas para investigar perfiles falsos: búsqueda inversa de imágenes de perfil en Google Imágenes o TinEye, revisión de la antigüedad del perfil, análisis de sus interacciones.

**Nivel 2: Intermedio (requiere coordinación con aliadas técnicas o formación adicional):**

- **Adquisición lógica de dispositivos móviles:** Si se cuenta con las herramientas y el conocimiento (y previo consentimiento informado de la sobreviviente), realizar una adquisición lógica de los datos del teléfono (copia de seguridad de los datos visibles al usuario) utilizando herramientas forenses básicas o incluso el propio sistema de respaldo del dispositivo.
- **Análisis de logs del sistema:** Revisar registros de eventos del sistema operativo (en computadoras) para identificar actividad sospechosa.
- **Análisis de tráfico de red básico:** En casos de sospecha de software espía, se podría, con el consentimiento y la ayuda de la sobreviviente, monitorear el tráfico de red de su dispositivo en busca de comunicaciones sospechosas (esto requiere más conocimiento y herramientas específicas).

**Nivel 3: Avanzado (derivación a perita forense):**

- Adquisición física de dispositivos.
- Análisis profundo de memoria volátil.
- Recuperación de archivos eliminados.
- Análisis de dispositivos con cifrado o dañados.
- Cualquier procedimiento que requiera la ruptura de un precinto o la modificación del estado original del dispositivo.

**Principio fundamental en todos los niveles:**

Consentimiento informado y progresivo. En cada paso, explicar a la sobreviviente qué se va a hacer, por qué, qué información se podría encontrar (incluyendo información personal no

relacionada con el caso) y qué medidas se tomarán para proteger su privacidad. Ella debe decidir si desea continuar.

### 2.3. Análisis legal y construcción de la estrategia

**Objetivo:**

Definir, junto con la sobreviviente, las acciones a seguir, considerando sus deseos, los hallazgos del análisis forense y el marco legal vigente**.**

**Acciones:**

***Asesoría legal (si está disponible): Consultar con la abogada aliada para:***

- Identificar los tipos penales aplicables (violencia informática, acoso, hostigamiento, amenazas, y la agravante por uso de TIC, según la Ley Orgánica sobre el Derecho de las Mujeres a una Vida Libre de Violencia).
- Evaluar la viabilidad de una denuncia penal y los pasos a seguir.
- Identificar medidas de protección que se pueden solicitar (prohibición de comunicación por cualquier medio, incluyendo digitales).
- Analizar la posibilidad de acciones civiles por daños y perjuicios.
- ***Presentación de escenarios:*** Exponer a la sobreviviente las diferentes opciones disponibles, explicando los pros y contras de cada una, los tiempos estimados y los posibles resultados. Los escenarios pueden incluir:
    - **Escenario 1:**
        - *Gestión ante plataformas:* Reportar los perfiles y contenidos abusivos a las redes sociales y plataformas para su eliminación (ver Anexo 1). Esto puede ser suficiente si el objetivo principal es que cese la agresión en línea.
    - **Escenario 2:**
        - *Denuncia penal:* Acudir al Ministerio Público u órgano receptor de denuncias para iniciar una investigación formal. Esto requiere una evidencia sólida y la disposición de la sobreviviente a participar en un proceso judicial que puede ser largo y, en ocasiones, revictimizante.
    - **Escenario 3:**
        - *Estrategia mixta:* Combinar la gestión ante plataformas con la denuncia penal.
    - **Escenario 4:**
        - *Medidas de autoprotección continuadas:* Implementar medidas de seguridad digital y contención sin recurrir a instancias formales, si la sobreviviente no desea hacerlo o si el caso no lo permite.
- **Toma de decisión:** Respetar la decisión de la sobreviviente. No presionar. Acompañar la opción que ella elija, por pequeña que parezca. Si decide no denunciar, apoyar esa decisión y trabajar en otras vías de reparación.

### 2.4. Preparación de la evidencia para la acción elegida

**Objetivo:**

Organizar y preparar la evidencia recopilada y analizada para que pueda ser utilizada de manera efectiva en la estrategia definida.

**Acciones:**

***Si la opción es gestión ante plataformas:***

- Tener a mano las capturas de pantalla, enlaces, metadatos y/o números de reporte.
- Utilizar las guías específicas de reporte para cada plataforma (Anexo 1).

***Si la opción es denuncia penal:***

Distinguir claramente entre "sistematización de la agresión" (nuestro cuadro) y "evidencia digital forense". Explicar a la sobreviviente que los PDFs y capturas de pantalla son un buen punto de partida y ayudan a narrar los hechos, pero que para un proceso judicial se requiere una cadena de custodia y un análisis forense que garantice la inmutabilidad de la evidencia.

Si se requiere un informe pericial y se cuenta con una perita aliada, facilitar el contacto y asegurar que la evidencia sea entregada siguiendo los protocolos establecidos (dispositivo original, sin alterar, con registro de cadena de custodia).

Si no se cuenta con perita, la evidencia sistematizada puede servir como base para la denuncia, pero se debe informar a la fiscalía de las limitaciones técnicas y solicitar que sean ellos quienes realicen la experticia correspondiente.


### 3.1. Acompañamiento continuo

**Objetivo:**

Mantener el contacto con la sobreviviente, monitorear la evolución del caso y brindar apoyo en las distintas fases del proceso elegido.

**Acciones:**

- ***Establecer una periodicidad de contacto:*** Acordar con la sobreviviente cada cuánto tiempo nos contactaremos (puede ser semanal, quincenal o mensual, según sus necesidades y la intensidad del caso). Dejar claro que ella también puede contactarnos en cualquier momento si surge alguna novedad o emergencia.

***Seguimiento de las acciones emprendidas:***

- ***Si se hicieron reportes a plataformas:*** preguntar si ha recibido respuesta, ayudarla a hacer seguimiento con el número de reporte, y si no hay respuesta, insistir en un nuevo reporte.
- ***Si se interpuso una denuncia:*** acompañarla a las citaciones si es posible y si ella lo desea, ayudarla a preparar la documentación requerida, brindar apoyo emocional antes y después de las comparecencias.
- ***Monitoreo de nuevas agresiones:*** Preguntar si ha habido nuevos episodios de violencia o si el agresor ha cambiado su modus operandi. Si es así, reiniciar el proceso de documentación.
- ***Apoyo en la implementación de medidas de autoprotección:*** Reforzar la importancia de mantener buenas prácticas de seguridad digital, ayudarla a actualizar contraseñas periódicamente, y estar atentas a posibles intentos de re-victimización.

### 3.2. Cuidados del equipo de acompañamiento

**Objetivo:**

Prevenir el desgaste emocional y el agotamiento de las personas que acompañan, reconociendo que el trabajo con violencia puede tener un alto impacto psicológico.

**Acciones:**

- ***Trabajo en equipo:*** No acompañar casos de forma aislada. Siempre que sea posible, que dos personas del equipo estén al tanto del caso para poder compartir la carga y apoyarse mutuamente.
- ***Reuniones de supervisión:*** Espacios periódicos donde el equipo pueda hablar de los casos, compartir cómo se sienten, identificar dificultades y buscar soluciones colectivas. Esto no es una terapia, sino un espacio de cuidado colectivo y aprendizaje compartido.
- ***Establecer límites:*** Reconocer que no podemos con todo. Aprender a decir "no" cuando un caso supera nuestras capacidades y derivar responsablemente.
- ***Rotación de casos:*** Si es posible, rotar los casos más complejos o desgastantes entre las integrantes del equipo.
- ***Tiempos de desconexión:*** Fomentar que cada integrante del equipo tenga sus propios espacios de autocuidado y desconexión del trabajo de acompañamiento.


### 4.1. Criterios para el cierre

**Objetivo:**

Determinar cuándo un caso puede considerarse cerrado, en acuerdo con la sobreviviente y los siguientes criterios posibles:

- La sobreviviente comunica que se siente satisfecha con los resultados obtenidos y no requiere acciones adicionales.
- Se logró la eliminación del contenido dañino de las plataformas.
- El proceso judicial (si lo hubo) ha concluido (con sentencia, archivo fiscal, etc.).
- La sobreviviente ha recuperado el control de sus cuentas y dispositivos y se siente segura.
- La sobreviviente decide, por cualquier motivo, no continuar con el acompañamiento.
- Después de un tiempo prolongado sin novedades y sin respuesta de la sobreviviente a los intentos de contacto, se considera que el caso está inactivo.

### 4.2. Proceso de cierre

**Acciones:**

- ***Conversación de cierre:*** Tener una reunión con la sobreviviente para revisar juntas el camino recorrido. Reconocer sus fortalezas, sus logros y el esfuerzo realizado. Validar sus emociones.
- ***Retroalimentación:*** Preguntar a la sobreviviente cómo vivió el proceso de acompañamiento, qué le sirvió, qué no, qué mejoraríamos. Esta información es valiosísima para la etapa de Revisión.
- ***Entrega de materiales:*** Si se generaron informes, guías personalizadas o cualquier otro documento durante el proceso, asegurarse de entregarlos a la sobreviviente en formato seguro.
- ***Puertas abiertas:*** Dejar claro que, aunque el caso se cierra, puede volver a contactarnos si surge una nueva situación o si necesita apoyo nuevamente en el futuro (aquí tomar en cuenta que la mayoría de los casos son recurrentes).
- ***Cifrado y archivo seguro de la documentación:*** Una vez cerrado el caso, asegurar que toda la documentación (anonimizada) se archive de forma segura y cifrada, en caso de que sea necesaria para futuras consultas o investigaciones.


### 5.1. Análisis colectivo del caso

**Objetivo:**

Reflexionar sobre el caso cerrado para identificar aprendizajes, buenas prácticas, dificultades y áreas de mejora, tanto a nivel técnico como de proceso.

**Acciones:**

- ***Reunión de equipo:*** Dedicar un espacio específico para revisar el caso (siempre preservando la confidencialidad y utilizando solo la información anonimizada).
- ***Preguntas guía para la reflexión:***
  - ¿Qué funcionó bien en el acompañamiento?
  - ¿Qué dificultades enfrentamos? ¿Cómo las resolvimos?
  - ¿Nuestro análisis digital fue adecuado? ¿Qué herramientas técnicas nos faltaron?
  - ¿La coordinación con la asesoría legal fue fluida?
  - ¿Cómo fue la experiencia emocional para el equipo? ¿Qué nos enseñó este caso sobre nuestros propios límites y necesidades de cuidado?
  - ¿La sobreviviente quedó satisfecha? ¿Qué aprendimos de su retroalimentación?
  - ¿Este caso nos muestra algún vacío en nuestro protocolo o en nuestras capacidades?

### 5.2. Actualización de herramientas y conocimientos

**Objetivo:**
Incorporar los aprendizajes de la revisión para mejorar la práctica futura y mantener actualizados los conocimientos técnicos y legales.

**Acciones:**

- ***Actualización del protocolo:*** Si se identifican mejoras, incorporarlas al protocolo.
- ***Identificación de necesidades de formación:*** A partir de las dificultades técnicas encontradas, identificar temas para futuros talleres o formaciones (ej. análisis de aplicaciones de mensajería, forénsica en iOS, uso de herramientas específicas como MVT, etc.).

- ***Investigación continua:*** Dedicar tiempo a investigar nuevas formas de violencia digital, nuevas herramientas y actualizaciones legales. Las VGFT mutan constantemente y nuestra respuesta debe estar en permanente evolución.
- ***Fortalecimiento de la red de aliadas:*** A partir de los casos, identificar necesidades de apoyo externo (abogadas especializadas en lo penal, peritas forenses, psicólogas con enfoque de género) y fortalecer los vínculos con estas profesionales u organizaciones.

# Referencias bibliográficas


Rojas, Jesús, (2026). Fundamentos de Informática Forense con Perspectiva Feminista *[Taller en línea]*. Mujeres Activistas XSL. Caracas, Venezuela.

Borrero Vásquez, Nazly (2024). *Cadena inmutable: Homologación y forensia en la era digital. Guía homologada de la cadena de custodia y forensia digital para jueces, fiscales, policías judiciales y abogados* (1.ª ed.). Edición del Autor.

Mujeres Activistas por el Software Libre (2022). *Guía 3: Lo que debes hacer en caso de ser víctima de violencias digitales*. Caracas, Venezuela. Recuperado de: https://activistasxsl.org/wp-content/uploads/2022/10/GUIA-3-ActivistasXSL.pdf

SocialTIC. (s. f.). *SocialTIC Forensics*. https://forensics.socialtic.org/index.html

# Anexos

**Anexo 1. Guía rápida de reporte en plataformas según Mujeres Activistas por el Software Libre (2022) presentado en su "Guía 3: Lo que debes hacer en caso de ser víctima de violencias digitales"**

**facebook**

| | |
|---|---|
| **¿Cómo reportar un post?** | • **Paso 1:** Hacer clic en los tres puntos (...) en la esquina superior derecha del post.<br>• **Paso 2:** Seleccionar Reportar publicación.<br>• **Paso 3:** Selecciona la categoría según su caso: Problema que involucra a un menor de 18 años; Bullying, acoso o abuso; Contenido para adultos. Dentro de estas, encontrarás opciones específicas como "Amenaza con compartir imágenes mías sin ropa" o "Explotación sexual".<br>• **Paso 4:** Finalizar haciendo clic en Enviar. |
| **¿Cómo reportar un perfil?** | • **Paso 1:** Ingresar al perfil que se desea reportar.<br>• **Paso 2:** Ubicar los tres puntos (...) que aparecen a la derecha.<br>• **Paso 3:** Seleccionar Buscar ayuda o reportar perfil.<br>• **Paso 4:** Selecciona la categoría que mejor describa el caso. Dentro de las opciones principales están: Problema que involucra a un menor de 18 años; Bullying, acoso o abuso; Contenido para adultos. Dentro de estas, encontrarás opciones críticas como "Amenaza con compartir imágenes mías sin ropa" o "Explotación sexual". Es fundamental elegir la opción más precisa para que el sistema de Facebook priorice el reporte adecuadamente. |
| **Si se tardan** | • **Paso 1:** Guardar el enlace de la publicación o del perfil como PDF en tu computadora o envíalo a un correo electrónico propio para asegurar su trazabilidad o realizar una captura de pantalla completa de la publicación o perfil reportado.<br>• **Paso 2:** Guardar el número de reporte para posteriormente solicitar avance del mismo.<br>• **Paso 3:** Realizar el seguimiento a través del "Buzón de ayuda" dentro de la configuración de Facebook. |

**Instagram**

| | |
|---|---|
| **¿Cómo reportar un post?** | • **Paso 1:** Toca los tres puntos (...) en la esquina superior derecha del post.<br>• **Paso 2:** Selecciona Reportar.<br>• **Paso 3:** ¿Por qué quieres reportar esta publicación? Elige Desnudos o actividad sexual (para imágenes íntimas); Bullying o contacto no deseado (si es hostigamiento), según el caso.<br>• **Paso 4:** Selecciona la opción más específica, como "Amenaza con compartir o comparte imágenes sin ropa".<br>• **Paso 5:** Toca en "Enviar reporte". |
| **Si se tardan** | • **Paso 1:** Guardar el enlace como PDF en tu computadora o realizar captura de pantalla.<br>• **Paso 2:** Guardar el número de reporte para posteriormente solicitar avance del mismo.<br>• **Paso 3:** Ve a Configuración > Ayuda > Solicitudes de ayuda > Reportes para ver el estado de tu reporte. |

## WhatsApp

| | |
|---|---|
| **Consideraciones Importantes (Antes de reportar)** | • **Reporta rápido:** Es fundamental hacerlo pronto para que WhatsApp pueda recibir y revisar los mensajes más recientes del chat como prueba.<br>• **Qué recibe WhatsApp:** Al reportar, la plataforma recibe los últimos 5 mensajes enviados por esa persona o grupo, pero no notifica al agresor que ha sido reportado.<br>• **Documenta primero:** Antes de reportar y bloquear, realiza capturas de pantalla de la conversación completa, ya que una vez bloqueado o si se borran los mensajes, podrías perder evidencia visual valiosa. |
| **Pasos para reportar** | • **Paso 1:** Abre el chat con la persona o el grupo que quieres denunciar.<br>• **Paso 2:** Toca el nombre del contacto o del grupo en la parte superior para ver su perfil.<br>• **Paso 3:** Desliza hasta el final y toca en Reportar contacto o Reportar grupo.<br>• **Paso 4:** Elige si quieres solo Reportar o Reportar y bloquear (se recomienda la opción de reportar y bloquear de inmediato). |

## Red Social

| | |
|---|---|
| **¿Cómo reportar un post?**<br><br>Recordar que X le da prioridad a las denuncias realizadas por la parte afectada | • **Paso 1:** Toca los tres puntos (...) en la esquina superior derecha del post.<br>• **Paso 2:** Selecciona "Denunciar post".<br>• **Paso 3:** En el menú "¿Qué quieres denunciar?", elige la opción que mejor describa la agresión:<br>  ◦ *Contenido privado o no consentido:* para imágenes íntimas, datos personales expuestos (Doxing) o fotos tuyas publicadas sin permiso).<br>  ◦ *Odio, abuso o acoso:* para insultos, hostigamiento sistemático o amenazas).<br>  ◦ *Protección de personas menores de edad*<br>  ◦ *Suplantación de identidad:* si usan tu nombre o fotos para crear una cuenta falsa y atacarte.<br>• **Paso 4:** Toca en el botón "Listo" para finalizar el reporte.<br>• **Paso 5:** Guarda el número de reporte que te llegue al correo. |
| **Si se tardan** | • **Paso 1:** Guardar el enlace como PDF en tu computadora o realizar captura de pantalla.<br>• **Paso 2:** Guardar el número de reporte para posteriormente solicitar avance del mismo. |

Google

| | |
|---|---|
| **¿A dónde ir?** | • **Paso 1:** Ingresa directamente a la herramienta de soporte de Google: Eliminar contenido de Google.<br>• **Paso 2:** Selecciona la opción **"Iniciar solicitud de eliminación"**. |
| **¿Cómo llenar el formulario?**<br><br>**Importante:** A diferencia de las redes sociales, reportar en Google sirve para desindexar (hacer desaparecer) el contenido de los resultados de búsqueda, lo cual es vital para reducir el alcance del daño en casos de VGFT) | • **Paso 1:** Elige el motivo (Material sexual o imágenes de desnudos, Información personal o Menores) y selecciona tu País.<br>• **Paso 2:** Describe tu situación (Imagen real, Montaje/Deepfake, Menores, entre otras).<br>• **Paso 3:** Pega los Links (URLs) directos del contenido ofensivo y de la imagen o video.<br>• **Paso 4:** Escribe los términos de búsqueda (ej. tu nombre) con los que aparece el contenido.<br>• **Paso 5:** Confirma quién aparece: selecciona "Soy yo" (o a quien representas).<br>• **Paso 6:** Describe brevemente el caso y sube capturas de pantalla de la agresión.<br>• **Paso 7:** Elige Anonimato (sin avisos) o Notificaciones (seguimiento por correo).<br>• **Paso 8:** Confirma que la información es verdadera. Firma escribiendo tu nombre completo (como en tu Cédula de Identidad) y haz clic en Enviar.<br>• **Paso 9:** Si no fue anónimo, guarda el número de caso que llegará a tu correo.<br><br>**Nota de seguridad:** Google solo borra el resultado de su buscador, pero no elimina la publicación original del sitio web. Es vital reportar también en la página o red social de origen. |
| **¿Datos necesarios?** | • **Nombre completo (firma legal).**<br>• **País**<br>• **URLs específicas:** El link directo del contenido y el link del resultado de búsqueda de Google donde aparezca la imagen o el vídeo.<br>• **Términos de búsqueda:** Palabras usadas para encontrar el contenido.<br>• **Capturas de pantalla del contenido ofensivo:** Evidencia del contenido para asegurarnos de retirar los resultados correctos (puedes censurar las partes más explícitas, pero debe seguir siendo reconocible para que Google pueda retirarlo)<br>• **Correo electrónico de contacto:** Para recibir el número de caso (obligatorio si no es anónimo). |

Estás son las plataformas de redes sociales más usadas actualmente, sin embargo también se puede reportar con procedimientos similares en otras redes sociales como OnlyFans y en plataformas de contenido pornográfico explícito como Youporn, Pornhub, entre otras.

## Anexo 2. Glosario de términos técnicos y legales

- **Cadena de custodia:** Procedimiento controlado que se aplica a la evidencia digital desde su localización hasta su valoración por los órganos judiciales, para garantizar su autenticidad, integridad e inmutabilidad.

- **Evidencia digital:** Información almacenada o transmitida en formato digital que puede ser utilizada como prueba en un proceso judicial.

- **Hash digital (MD5, SHA-256):** Algoritmo matemático que genera un valor único (una "huella digital") para un archivo o conjunto de datos. Cualquier modificación en el archivo original genera un hash diferente. Sirve para verificar la integridad de la evidencia.

- **Informática forense:** Conjunto de procedimientos y técnicas para identificar, recolectar, preservar, analizar y presentar evidencia digital de manera que sea aceptable en un proceso legal.

- **Perito informático forense:** Persona experta en informática forense, capacitada para realizar investigaciones y presentar informes periciales ante tribunales.

- **Stalkerware:** Software malicioso, a menudo instalado sin consentimiento en dispositivos móviles, que permite a una persona monitorear la actividad de la víctima (ubicación, mensajes, llamadas, actividad en redes sociales).

- **Doxeo (Doxing):** La práctica de investigar y publicar información privada o identificable sobre una persona en internet, generalmente con fines maliciosos.

- **Violencia informática:** Tipo de violencia contra las mujeres definido en la Ley Orgánica sobre el Derecho de las Mujeres a una Vida Libre de Violencia, que incluye la divulgación de información o imágenes de carácter íntimo sin consentimiento, acoso a través de TIC, entre otros.

## Anexo 3. Modelo de consentimiento informado para análisis forense

### CONSENTIMIENTO INFORMADO PARA ANÁLISIS FORENSE

Yo, _____, titular de la cédula de identidad N° _____, en el marco del acompañamiento brindado por [Nombre de la organización], otorgo mi consentimiento libre, informado y voluntario para que se realicen las siguientes acciones sobre mis dispositivos y cuentas digitales, con el único fin de documentar y analizar las violencias de las que he sido víctima:

Se me ha explicado de manera clara y comprensible que:

1. **Qué se hará:** Se realizará una revisión básica de mis dispositivos y/o cuentas para identificar evidencia de la agresión (mensajes, imágenes, registros de actividad sospechosa, aplicaciones no deseadas). Esto puede incluir la revisión de capturas de pantalla, la descarga de archivos de datos de mis cuentas y la inspección visual de mi teléfono.
2. **Por qué es necesario:** Esta revisión permitirá comprender mejor la naturaleza del ataque, identificar al agresor y fortalecer las acciones que decidamos emprender (reportes a plataformas, denuncia legal, etc.).
3. **Qué información se podría encontrar:** Durante la revisión, podría encontrarse información personal no relacionada con el caso. Se tomarán todas las medidas para respetar mi privacidad y no se utilizará ni divulgará dicha información.
4. **Medidas de confidencialidad:** Toda la información revisada será tratada de forma estrictamente confidencial. Mis datos personales serán anonimizados y los archivos se almacenarán de forma cifrada.
5. **Límites de esta revisión:** Esta revisión es básica y no constituye un peritaje forense profesional. No se modificará ni alterará el estado original de mis dispositivos a menos que yo lo autorice expresamente para un paso posterior.
6. **Derecho a revocar:** Puedo revocar este consentimiento en cualquier momento, sin necesidad de dar explicaciones y sin que ello afecte el acompañamiento que recibo.

En consecuencia, AUTORIZO la realización de las acciones descritas.